THEOREMS ON SIMPLE GROUPS*

BY

H. F. BLICHFELDT

Introduction and Terminology.

§ 1. It is our purpose in this paper to state and prove a somewhat more precise theorem on simple groups than that given by FROBENIUS in his article *Ueber auflösbare Gruppen. V.*† This theorem of FROBENIUS we shall state in the following form: "Let H be a group whose order is divisible by p^λ, p being a prime. If H is simple, then there is in H a substitution T_1 whose order is prime to p, which is commutative with some subgroup Q of H of order p^μ and not commutative with every subgroup of Q. In the contrary case, H has an invariant subgroup of index p^λ, containing all the substitutions of H whose orders are prime to p."

The theorem which we shall here establish (divided for convenience into four parts, I, II, III, IV) defines the group Q more explicitly, and the nature of the relation of T_1 to Q in the most important case, namely, when Q is a Sylow subgroup of H. Several applications are added in the form of corollaries.

The phraseology of ordinary group theory will be employed. The following abbreviations are used:

$A = B$ means "the groups (substitutions) A and B are identical";

$A < B$ means "the group (substitution) A is contained in the group B, though it is not identical with B."

The letters H, P, P_1 and T have the following significance throughout:

H represents a group of order $p^\lambda n$, p being a prime number not dividing n;

P represents any given subgroup of H of order p^λ;

P_1 represents any given subgroup of P of order $p^{\lambda-1}$; and

T is the general symbol for a substitution of H whose order is prime to p.

Though it is contrary to general usage, we shall proceed from right to left in a succession of substitutions indicated. A function subjected to a substitution or a succession of such shall be written to the right of the substitutions indi-

* The present paper is an extension of two papers read before the San Francisco section, viz., *A theorem concerning the Sylow subgroups of simple groups*, September 29, 1906; and *A theorem on simple groups*, September 26, 1908.

† Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin, 1901, p. 1324.

cated, enclosed in parentheses. Thus, if A and B represent substitutions, I a function, the symbol $AB(I)$ represents the function obtained by first subjecting I to the substitution B, and then subjecting the result to the substitution A.

Theorems and corollaries.

§ 2. **Theorem I.** *Among the substitutions contained in P, but not in P_1, let S be any one of those of lowest order. Then, if H is simple, there are in H a group Q (either $= P$ or $< P$, containing S) and a substitution T, say T_1, of the following nature:*

1°) *If $Q = P$, this substitution T_1 is commutative with P but not with S; more generally, the commutator $S^{-1}T_1^{-1}ST_1$ is not in P_1.*

2°) *If $Q < P$, then T_1 is commutative with Q, but not with every subgroup of Q of index p.*

Theorem II. *If $Q < P$, there is a group $Q_1 \leqq Q$ containing S, and there is a certain series of groups*

$$Q_1,\ Q_2,\ Q_3,\ \cdots,\ Q_{\lambda-\nu+1} = P$$

of orders p^ν, $p^{\nu+1}$, $p^{\nu+2}$, $\cdots$, p^λ, respectively, each a subgroup of the one to the right of it, possessing the following property. Let R_i be that group whose substitutions are common to all the subgroups of Q_i of index p. Then, if A_i be any substitution of Q_i but not of Q_{i-1}, $i > 1$, the substitution

$$(SA_i)^p A_i^{-p},$$

though a substitution of Q_{i-1}, does not belong to R_{i-1}.

Corollary 1. *Every substitution of P commutative with S must belong to Q.* More generally, if $p > 2$, every substitution A of P, such that the substitutions A and SAS^{-1} are commutative, must belong to Q. Hence, *if $p > 2$, every abelian subgroup of P which is transformed into itself by S, must belong to Q.*

We prove this corollary from Theorem II by making use of the facts that R_{i-1} is invariant in Q_i; that every commutator of Q_{i-1} belongs to R_{i-1}; that the pth powers of the substitutions of Q_{i-1} belong to R_{i-1}.

Theorem III.

α) *If $Q_1 < P$, then the order p^λ of P is $\geqq p^{p+1}$, or is $\geqq p^{p^2}$, according as the order of Q_1 is $= p^{\lambda-1}$, or is $< p^{\lambda-1}$.*

β) *If the order of P is $< p^{2p-1}$, then there is in P some subgroup P_1 and substitution S for which the corresponding group $Q = P$.*

Corollary 2. *The group Q is certainly $= P$ in the cases where P*

1°) *is abelian* (Theorem II),

2°) *or contains no substitutions of order p^2* (Theorem II),

3°) *or is of order p^p at most* (Theorem III).

In any of these cases H will therefore contain a subgroup M which contains P invariantively. Any one of the substitutions S of P (defined in Theorem I) is non-commutative with some substitution T of M.

In particular, if P fulfills both 1°) and 2°), then no one of its substitutions (except identity) is invariant in M.

Corollary 3. *Let p be the lowest prime which divides the order of A, and let it be given that the corresponding subgroup P is abelian.* Let a set of independent generating substitutions of P be constructed; then, if one of these generators be of order p^a, there must be at least three generators of order p^a if $p > 2$; at least two if $p = 2$.*

Hence, if $p > 2$, and if the order of P be $\leqq p^8$, then P must be of type $(1, 1, \cdots, 1)$ in every case, with the exception of the possibility $(2, 2, 2)$. Again, if $p = 2$, and the order of P be $\leqq p^6$, the only permissible types are the following: $(1, 1)$, $(1, 1, 1)$, $(1, 1, 1, 1)$, $(1, 1, 1, 1, 1)$, $(1, 1, 1, 1, 1, 1)$, $(2, 2)$, $(2, 2, 1, 1)$, $(2, 2, 2)$, $(3, 3)$.

To prove this corollary, let A_1, A_2, $\cdots$ be the generators of order p^a; B_1, B_2, $\cdots$ the generators whose orders, p^{b_1}, p^{b_2}, $\cdots$ are $> p^a$. The group K, generated by the substitutions $B_1^{p^{b_1-1}}$, $B_2^{p^{b_2-1}}$, $\cdots$, $A_1^{p^{a-1}}$, $A_2^{p^{a-1}}$, $\cdots$, is a characteristic subgroup of P.† Moreover, the group K', generated by $B_1^{p^{b_1-1}}$, $B_2^{p^{b_2-1}}$, $\cdots$ (leaving out of K the generators $A_1^{p^{a-1}}$, $\cdots$), is a characteristic subgroup of P. Let the factor-group K/K' be denoted by L, and its generating substitutions by a_1, a_2, $\cdots$, corresponding to A_1, A_2 $\cdots$.

In applying Theorem I, 1°), let P_1 be that group generated by those generators of P whose orders are higher or lower than p^a, and by A_1^p, A_2, $\cdots$. Then we may put $S = A_1$, and we must have

$$T_1^{-1} A_1 T_1 = A_1^x C, \qquad x \not\equiv 1 \pmod{p},$$

where C belongs to P_1.

Accordingly,

$$T_1^{-1} A_1^{p^{a-1}} T_1 = (A_1^{p^{a-1}})^x C^{p^{a-1}}.$$

Since T_1 is commutative with L, we have correspondingly

$$T_1^{-1} a_1 T_1 = a_1^x c,$$

c belonging to that subgroup of L generated by a_2, $\cdots$. Hence, if there were only two generators, a_1, a_2, in L, then the order of T_1 would be a factor of $p^2 - 1$. But this number is divisible by no prime $> p$ except when $p = 2$.

* The more general case where P is not abelian, if it be only such that, for every P_1 and S, $Q = P$ (cf. Cor. 2), is embodied in this corollary when B_1, $\cdots$, A_1, $\cdots$, instead of being the generators of P, are the generators of the factor-group P/W, W being the commutator subgroup of P.

† FROBENIUS, *Ueber auflösbare Gruppen.* II, Sitzungsberichte der Akademie der Wissenschaften zu Berlin (1895), pp. 1028–1029. BURNSIDE, *Theory of Groups*, pp. 233–235.

At the end of his paper on soluble groups, referred to in the introduction,* FROBENIUS proves that every group of order $p^\lambda qr$ is soluble, if $\lambda \leqq 4$; p, q, r being odd primes. Using his arguments in conjunction with Theorems I–III we find the

Corollary 4. *Every group of order $p^\lambda qr$ is soluble, if $\lambda \leqq p^2 - 1$; p, q, r being different odd primes.*

Theorem IV. *If the conditions as specified for a simple group H in Theorems* I, II *and* III *are not all fulfilled with reference to S and P, then H has an invariant subgroup H_1 of index p, which does not contain S, but contains every substitution T of H.*

Proof of the theorems.

§ 3. Let P' be the largest subgroup of H whose substitutions are commutative with P, and which, besides, transform S into itself or into $S\times$ (a substitution of P_1). This group P' is of order $p^\lambda n'$, n' being a factor of n. We shall prove that

A) *The group P' contains an invariant subgroup P_1' of order $p^{\lambda-1}$, to which S does not belong; further, no substitution of P, not belonging to P_1', is of lower order than S.*

We write P' as a regular group in $p^\lambda n'$ letters

$$x_1,\ x_2,\ \cdots,\ x_{p^\lambda n'}.$$

The substitutions of P_1 will transform x_1 into $p^{\lambda-1}$ different letters, say

$$x_1,\ x_2,\ \cdots,\ x_{p^{\lambda-1}}.$$

The functions

$$I_1 = x_1 + x_2 + \cdots + x_{p^{\lambda-1}},\ S(I_1),\ S^2(I_1),\ \cdots,\ S^{p-1}(I_1) \tag{1}$$

are all absolute invariants for the group P_1. Let θ be a root different from 1, of the equation

$$\theta^p - 1 = 0,$$

and let us consider the function

$$I_2 = I_1 + \theta^{-1}S(I_1) + \theta^{-2}S^2(I_1) + \cdots + \theta^{-p+1}S^{p-1}(I_1).$$

It is not identically zero, no two of the functions (1) containing the same letter x_i. It is an absolute invariant for the group P_1, and we have

$$S(I_2) = \theta I_2.$$

We shall introduce the following abbreviations:

ζ means a power of θ; and

* Loc. cit., p. 1329.

ϕ means a power of θ, different from 1.

Then if A is any substitution of P,

$$A(I_2) = \zeta I_2, \qquad S(I_2) = \phi I_2.$$

§ 4. When the group P' is written symbolically in the form

$$P' = P + B_2 P + B_3 P + \cdots + B_{n'} P,$$

the function

$$I_3 = I_2 \cdot B_2(I_2) \cdot B_3(I_2) \cdot \cdots \cdot B_{n'}(I_2) \tag{2}$$

is seen to be a relative invariant for P'. We find that

$$S(I_3) = \theta^{n'} I_3 = \phi I_3.$$

It follows that all the substitutions of P' for which I_3 is an absolute invariant form an invariant subgroup P'' of order $p^{\lambda-1}n'$, not containing S. This subgroup has a subgroup P_1' of order $p^{\lambda-1}$, also invariant in P'. The first part of (A), § 3, has thus been proved.

To prove the second part, we remark first that, as P is invariant in P', all the factors of I_3 are relative invariants for P. Hence, if A be a substitution of P and not of P_1', the condition

$$A(I_3) = \phi I_3$$

necessitates that, for some factor $B_i(I_2)$ of the right-hand member of (2), the relation shall subsist:

$$AB_i(I_2) = \phi B_i(I_2).$$

This gives

$$B_i^{-1} A B_i(I_2) = \phi I_2.$$

It follows that $B_i^{-1}AB_i$, though a substitution of P, does not belong to P_1. Hence its order is not lower than that of S (cf. Theorem I). Hence the order of A is not lower than that of S.

§ 5. We shall now write H as a regular group in $h = p^\lambda n$ letters, $x_1, x_2, \cdots, x_h$. The substitutions of P'' will transform x_1 into $p^{\lambda-1}n'$ letters, say $x_1, x_2, \cdots, x_{p^{\lambda-1}n'}$. Let $I = x_1 + x_2 + \cdots + x_{p^{\lambda-1}n'}$, and let us consider the function

$$J = I + \theta^{-1}S(I) + \theta^{-2}S^2(I) + \cdots + \theta^{-p+1}S^{p-1}(I),$$

which is not identically zero.

B) *The group P' contains all the substitutions of H for which J is a relative invariant.*

Let W transform x_a into x_b, both occurring in J. Since the letters involved in J form a transitive set for the group P', we can find a substitution in the latter, say V, which also transforms x_a into x_b. The substitution VW^{-1} will

therefore leave x_b unchanged. Since H is written in regular form, it follows that VW^{-1} is identity. *If J be a relative invariant for W, and the order of W be a power of p, then W belongs to P.*

§ 6. The substitutions of H will transform J into n/n' expressions that do not differ by constant factors merely. The product π of these factors will be a relative or absolute invariant for H. Evidently, $A(\pi) = \zeta\pi$, A being any substitution of H. If

$$S(\pi) = \phi\pi,$$

then H contains an invariant subgroup H_1 of index p, consisting of all the substitutions C for which

$$C(\pi) = \pi.$$

To this subgroup would belong every substitution T of H. Accordingly, *unless the group H_1 of Theorem IV exists, we must have*

$$S(\pi) = \pi. \tag{3}$$

§ 7. To examine the nature of the factors of π, let us write H symbolically in the form

$$H = P' + PV_1 + PV_2 + \cdots + PV_{n-n'}. \tag{4}$$

The group P', operating upon J, will furnish just one of the factors of π, namely J. The p^λ substitutions represented by the symbol PV_i will furnish, say, p^{k_i} factors of π, whose product we shall indicate by π_i. Now, for $j \neq i$, one of the factors of π_j may be equal, apart from a constant multiplier, to one of the factors of π_i. In such a case we find $\pi_j = \pi_i \times$ (a constant). We shall then agree to say that $\pi_j = 1$, if $j > i$. With this understanding we may write

$$\pi = J\pi_1\pi_2 \cdots \pi_{n-n'}.$$

Since $S(J) = \theta J$, $S(\pi_i) = \zeta\pi_i$, it follows that, if (3) is to hold, there is at least one index ρ such that

$$S(\pi_\rho) = \phi\pi_\rho. \tag{5}$$

§ 8. First, let π_ρ consist of a single factor. Then the alternative case 1°) of Theorem I is proved in the following manner. Let V be one of the substitutions PV_ρ of (4). Then we may suppose that

$$\pi_\rho = V(J).$$

The function π_ρ is here a relative invariant for P. Hence, J is a relative invariant for $V^{-1}PV$. Hence, by (B), § 5,

$$V^{-1}PV = P.$$

Now, since V does not belong to P', the group generated by V and P', though containing P invariantively, does not fulfill the other conditions imposed upon P' in § 3. Case 1°) of Theorem I thus follows.

§ 9. Next, let π_ρ consist of more than one factor,

$$\pi_\rho = y_1 y_2 \cdots y_{p^k}. \tag{6}$$

C) Then we shall prove that V, *one of the substitutions of the symbol* PV_ρ, *transforms a certain subgroup* Q_1 *of* P, *which contains* S, *into itself or into another subgroup of* P. *Moreover,* V *does not transform that subgroup of* Q_1 *which is also a subgroup of* P_1' *into itself or into another subgroup of* P_1'.

Substituting (6) in (5), it might happen that, for some index j, we have $S(y_j) \neq \zeta y_j$. Then we may suppose that

$$S(y_j) = y_{j+1},\ S(y_{j+1}) = y_{j+2},\ \cdots,\ S(y_{j-1+p^l}) = \theta' y_j \qquad (\theta'^p = 1).$$

Thus, if $y_j = W(J)$, we get

$$W^{-1} S^{p^l} W(J) = \theta' J. \tag{7}$$

Hence (§ 5, B) $W^{-1} S^{p^l} W < P$.

This substitution, being of lower order than S, must belong to P_1' (§ 3, A). The function J is, however, an absolute invariant for P'' and therefore for P_1' (cf. §§ 4, 5). Accordingly $\theta' = 1$.

§ 10. The p^k factors of π_ρ (6), permuted transitively by P, fall into p sets of p^{k-1} factors each, forming imprimitive sets. Let the p products of the factors of these sets be indicated by

$$a_1,\ a_2,\ \cdots,\ a_p; \qquad a_1 a_2 \cdots a_p = \pi_\rho.$$

Substituting in (5), either we have

$$S(a_i) = \zeta a_i \qquad (i = 1, 2, \cdots, p); \tag{8}$$

or we may put

$$S(a_1) = a_2,\ S(a_2) = a_3,\ \cdots,\ S(a_p) = \phi a_1.$$

The latter relations would, however, lead to an equation like (7), $\theta' \neq 1$, contrary to what was proved in § 9. Accordingly, (8) is true, and $\zeta = \phi$ for some index i, say $i = 1$:

$$S(a_1) = \phi a_1. \tag{9}$$

That subgroup of P for which $a_1, a_2, \cdots, a_p$ are relative invariants shall be designated by $Q_{\lambda-\nu}$, where $\nu = \lambda - k$. Its order is $p^{\lambda-1}$.

The p^{k-1} factors of a_1 fall into p sets of imprimitivity for the group $Q_{\lambda-\nu}$. The respective products shall be indicated by

$$b_1,\ b_2,\ \cdots,\ b_p; \qquad b_1 b_2 \cdots b_p = a_1.$$

We may assume that $S(b_1) = \phi b_1$. The factors $b_1, b_2, \cdots, b_p$ are relative invariants for a group $Q_{\lambda-\nu-1} < Q_{\lambda-\nu}$, of order $p^{\lambda-2}$. Proceeding thus, we finally arrive at groups Q_3, Q_2, Q_1, of orders $p^{\nu+2}$, $p^{\nu+1}$, p^{ν} respectively, having sets of relative invariants respectively designated by

$$w_1, w_2, \cdots, w_p; \qquad v_1, v_2, \cdots, v_p; \qquad y_1, y_2, \cdots, y_p.$$

These invariants satisfy the relations

$$w_1 = v_1 v_2 \cdots v_p; \qquad v_1 = y_1 y_2 \cdots y_p.$$

It will be noticed that S belongs to all of these groups, and we have, corresponding to (9),

$$S(w_1) = \phi w_1, \; S(v_1) = \phi v_1, \; S(y_1) = \phi y_1.$$

§ 11. Let $y_1 = V(J)$, V being one of the p^λ substitutions PV_ρ [(4), § 7]. Then J is a relative invariant for the group $V^{-1} Q_1 V$, which must therefore be a subgroup of P (§ 5). The first statement in (C), § 9, is thus true.

Let A be a substitution of Q_2, but not of Q_1. Then we may suppose that

$$y_i = A^{-i+1}(y_1) \qquad (i = 2, \cdots, p);$$

and we get

$$(10) \quad \begin{aligned} \phi &= \frac{S(v_1)}{v_1} = \frac{S(y_1)}{y_1} \cdot \frac{S(y_2)}{y_2} \cdots = \frac{S \cdot ASA^{-1} \cdot A^2SA^{-2} \cdot \cdots \cdot A^{p-1}SA^{-p+1}(y_1)}{y_1} \\ &= \frac{(SA)^p A^{-p}(y_1)}{y_1} = \frac{V^{-1}(SA)^p A^{-p} V(J)}{J}. \end{aligned}$$

Now $(SA)^p A^{-p} < Q_1$, and is also contained in every subgroup of P of order $p^{\lambda-1}$. It is therefore contained in P_1'. For this group J is an absolute invariant. Therefore, if the second part of (C), § 9, were not true, then (10) could not be true.

§ 12. We shall now prove case 2°) of Theorem I. Let $Q^{(0)}$ be any subgroup of P such that $Q^{(0)} \geqq Q_1$, and let

$$(11) \qquad Q^{(0)}, Q^{(1)}, Q^{(2)}, \cdots, Q^{(n)} = P$$

be that series of groups in which each member is the largest subgroup of P containing the one immediately to the left of it invariantively. If H contains a substitution T which is commutative with one of these groups, say $Q^{(m)}$, $m > 0$, without being commutative with $Q^{(m-1)}$, then 2°) of Theorem I is true; the group Q in the theorem representing a certain group $> Q^{(m-1)}$ and $\leqq Q^{(m)}$. We shall therefore assume that every substitution P which is commutative with $Q^{(m)}$ of (11), or of any similar series, is commutative also with Q^{m-1}, $m > 0$. Under

this assumption the following theorem by Frobenius holds: If K represents the greatest subgroup of H in which $Q^{(k)}$ is invariant ($n > k \geqq 0$), then $Q^{(k+1)}$ is a Sylow subgroup of K.*

D) By means of this theorem we can prove that, *if V be the substitution considered in §§ 9, 11, we may write*

$$V = W_1 W_2 W_3 \cdots W_r,$$

where W_1, W_2, $\cdots$, W_r are substitutions of H, respectively commutative with the following members of a certain series of groups:

$$(12) \qquad L_1 = Q_1,\ L_2,\ L_3,\ \cdots,\ L_r = P,$$

each a subgroup of those that follow.

§ 13. To prove (D), let $VPV^{-1} = M$. Then M and P have in common the group Q_1, but no greater group. Let Q_1' be the greatest subgroup of P containing Q_1 invariantively, and Q_1'' the corresponding subgroup of M. The groups Q_1' and Q_1'' will generate a group N in which Q_1' is a Sylow subgroup by Frobenius's theorem, § 12. There is therefore in N a substitution W_1 such that $Q_{1,1} = W_1^{-1} Q_1'' W_1 \leqq Q_1'$, $Q_{1,1} > Q_1$. We have also $W_1^{-1} Q_1 W_1 = Q_1$. Let now $(W_1^{-1} V) P (W_1^{-1} V)^{-1} = M_1$. Then P and M_1 have in common a subgroup, say L_2, $\geqq Q_{1,1}$, and therefore $L_2 > Q_1$. If $L_2 = P$, then (D) is proved, the series (12) consisting of the two terms Q_1, P; in this case we find

$$V = W_1 W_2,$$

where W_2 is a certain substitution of H commutative with P.

If $L_2 < P$, let L_2' be the largest subgroup of P containing L_2 invariantively, L_2'' the corresponding subgroup of M_1. The groups L_2' and L_2'' generate a group in which L_2' is a Sylow subgroup, etc. Proceeding as above, the proof of (D) may be completed without difficulty.

§ 14. To complete the proof of case 2°) of Theorem I, let us consider the substitutions W_1, W_2, $\cdots$, W_r, respectively commutative with the groups of (12). If they were at the same time commutative with the corresponding subgroups of P_1', i. e., if W_i, which is commutative with L_i, is also commutative with that subgroup (L_i^0) of L_i which is a subgroup of P_1', then (C), § 9, would not be true. For, the group

$$V^{-1} L_1^0 V = W_r^{-1} \{ \cdots [W_2^{-1} (W_1^{-1} L_1^0 W_1) W_2] \cdots \} W_r$$

* Paper referred to in § 1, p. 1325, Lemma I. The above theorem is apparently more general than that given by FROBENIUS, account being taken of the underlying assumptions as stated in both places. The method of proof by FROBENIUS is valid for the case considered here.

would then be a subgroup of P_1'. Accordingly, for some subscript i, there is a substitution, W_i, commutative with L_i, but not with L_i^0.

Now if G be the largest subgroup of H in which L_i is invariant, then L_i' is a Sylow subgroup of G (§§ 12, 13). Evidently, L_i^0 is invariant in L_i'. Since L_i^0 is not invariant in G (W_i belongs to G), it follows that there is a substitution T in G which is not commutative with L_i^0. The group L_i takes the place of Q in Theorem I, 2°).

§ 15. To prove Theorem II, let

$$Q_1,\ Q_2,\ \cdots,\ Q_{\lambda-\nu},\ P$$

be the series of groups arrived at in § 10. Let $A_{\lambda-\nu+1}$ be a substitution belonging to P, but not to $Q_{\lambda-\nu}$. Then we may suppose that

$$a_i = A_{\lambda-\nu+1}^{-i+1}(a_1) \qquad (i=2,3,\cdots,p).$$

We obtain

$$\phi = \frac{S(\pi_\rho)}{\pi_\rho} = \frac{1}{a_1}\,[S\cdot A_{\lambda-\nu+1}SA_{\lambda-\nu+1}^{-1}\cdot A_{\lambda-\nu+1}^{2}\,SA_{\lambda-\nu+1}^{-2}\cdot\cdots\cdot(a_1)]$$

$$= \frac{1}{a_1}\,(SA_{\lambda-\nu+1})^p A_{\lambda-\nu+1}^{-p}(a_1).$$

The function a_1, being a relative invariant for $Q_{\lambda-\nu}$, is plainly an absolute invariant for the group $R_{\lambda-\nu}$, whose substitutions are common to all the subgroups of $Q_{\lambda-\nu}$ of order $p^{\lambda-2}$. It follows that $(SA_{\lambda-\nu+1})^pA_{\lambda-\nu+1}^{-p}$ does not belong to $R_{\lambda-\nu}$.

Starting now with a substitution $A_{\lambda-\nu}$ belonging to $Q_{\lambda-\nu}$ but not to $Q_{\lambda-\nu+1}$, we may suppose

$$b_i = A_{\lambda-\nu}^{-i+1}(b_1) \qquad (i=2,3,\cdots,p).$$

Substituting in $\phi = S(a_1)/a_1$, we find that $(SA_{\lambda-\nu})^p A_{\lambda-\nu}^{-p}$ does not belong to $R_{\lambda-\nu-1}$, etc.

The group Q_1 is $\leqq Q$ of Theorem I, 2°), by §§ 12–14.

§ 16. We proceed to prove Theorem III. Considering the groups $Q_1, Q_2, \cdots, P$ of § 10, let A designate a substitution belonging to Q_2, but not to Q_1. We will assume that A permutes the letters $y_1, y_2, \cdots, y_p$ in the order

$$A: \qquad (y_1y_2\cdots y_p),$$

and that

$$S(y_i) = \theta^{\alpha_i}(y_i) \qquad (i=1,2,\cdots,p).$$

Then, since $S(v_1)=\phi v_1$,

$$\alpha_1+\alpha_2+\cdots+\alpha_p \not\equiv 0 \pmod p.$$

We shall say that *the constants $\theta^{\alpha_1}, \theta^{\alpha_2}, \ldots, \theta^{\alpha_p}$ are the multipliers of S.*

The substitution

$$S' = S^{x_1} \cdot A^{-1} S^{x_2} A \cdot A^{-2} S^{x_3} A^2 \cdot \cdots \cdot A^{-p+1} S^{x_p} A^{p-1},$$

belonging to Q_1, will have the multipliers θ, 1, 1, $\cdots$, 1, provided the congruences

$$\begin{aligned} \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_p x_p &\equiv 1, \\ \alpha_2 x_1 + \alpha_3 x_2 + \cdots + \alpha_1 x_p &\equiv 0, \\ \cdots\cdots\cdots\cdots & \\ \alpha_p x_1 + \alpha_1 x_2 + \cdots + \alpha_{p-1} x_p &\equiv 0 \pmod{p} \end{aligned}$$

are satisfied. The necessary condition is that the determinant Δ of the coefficients does not vanish (mod p). We find

$$\begin{aligned} \Delta &= (\alpha_1 + \theta\alpha_2 + \theta^2\alpha_3 + \cdots)(\alpha_1 + \theta^2\alpha_2 + \theta^4\alpha_3 + \cdots)\cdots \\ &\equiv \Delta^p \equiv (\alpha_1^p + \alpha_2^p + \alpha_3^p + \cdots)^p \equiv \alpha_1 + \alpha_2 + \alpha_3 + \cdots \not\equiv 0 \pmod{p}. \end{aligned}$$

The substitutions S', $A^{-1}S'A$, $A^{-2}S'A^2$, $\cdots$, all belonging to Q_1, are readily seen to generate a group of order p^p at least. The group Q_2 is accordingly of order p^{p+1} at least. Theorem III, α), is thus true when $Q_2 = P$.

§ 17. Let $Q_2 < P$. The functions v_1, v_2, $\cdots$, v_p (§ 10) contain p^2 factors y_1, y_2, $\cdots$. We may assume that

$$v_i = y_{(i-1)p+1}\, y_{(i-1)p+2} \cdots y_{ip} \qquad (i = 1, 2, \cdots, p).$$

We shall say that *the p factors of v_i constitute the set V_i*. The letter B shall designate a substitution belonging to Q_3 but not to Q_2. It permutes the letters v_1, v_2, $\cdots$, v_p in some such order as

$$B: \qquad (v_1 v_2 \cdots v_p).$$

Let R represent a substitution of the group Q_2. It has v_i for a relative invariant. We may assume that it permutes the members of the set V_i in the order $(y_{(i-1)p+1}\, y_{(i-1)p+2} \cdots y_{ip})$, or some power of this order,

$$R: \qquad (y_{(i-1)p+1}\, y_{(i-1)p+2} \cdots y_{ip})^n.$$

If $n = p$, i. e., if the functions $y_{(i-1)p+1}$, $\cdots$ are relative invariants for R, we shall say that *R is linear in V_i*. Otherwise we shall say that *R is circular in V_i*. Thus, S is linear in V_1, and A is circular in V_1.

§ 18. Let us now suppose that R is linear in V_i and write

$$R(y_{(i-1)p+j}) = \theta^{\beta_j} y_{(i-1)p+j} \qquad (j = 1, 2, \cdots, p).$$

We shall say that R *is of rank* m *in* V_i *if* $\beta_1 + \theta\beta_2 + \theta^2\beta_3 + \cdots + \theta^{p-1}\beta_p$ *is divisible by* $(1-\theta)^m$, *but by no higher power of* $1-\theta$; $\beta_1, \beta_2, \cdots, \beta_p$ *not being all equal* (*mod* p). *If* $\beta_1 \equiv \beta_2 \equiv \cdots \equiv \beta_p \not\equiv 0$ (*mod* p), *we shall say that* R *is of rank* $p-1$; *if* $\beta_1 \equiv \beta_2 \equiv \cdots \equiv \beta_p \equiv 0$ (*mod* p), *we shall say that* R *is of rank* p.

Let A_1 be any substitution contained in Q_2. Then $A_1 R A_1^{-1} R^{-1}$ is linear in V_i. It is of rank p if A_1 is linear in V_i; if A_1 is circular, the commutator in question is of rank $m+1$ if $m < p$, and of rank p if $m = p$.

§ 19. We can construct by the method of § 16, using S and B, a substitution S_1, $< Q_2$, such that

$$S_1(v_1) = \theta v_1, \qquad S_1(v_i) = v_i \qquad (i=2, 3, \cdots, p).$$

The following three cases may arise:

(1) S_1 is linear in $V_1, V_2, \cdots, V_p$;
(2) S_1 is circular in $V_1, V_2, \cdots, V_p$;
(3) S_1 is partly linear and partly circular.

Consider case (1). The substitution S_1 is of rank 0 in V_1 and of rank $\geqq 1$ in $V_2, V_3, \cdots, V_p$. The substitution $S_2 = AS_1A^{-1}S_1^{-1}$ is of rank 1 in V_1 and of rank $\geqq 2$ in $V_2, V_3, \cdots$. The substitution $S_3 = AS_2A^{-1}S_2^{-1}$ is of rank 2 in V_1 and of rank $\geqq 3$ in $V_2, V_3, \cdots$. Proceeding thus, we get a series of substitutions of which the last, $S_p = AS_{p-1}A^{-1}S_{p-1}^{-1}$, is of rank $p-1$ in V_1 and of rank p in $V_2, V_3, \cdots$.

The substitutions

$$S_p, \; BS_pB^{-1}, \; B^2S_pB^{-2}, \; \cdots, \; B^{p-1}S_pB^{-p+1}$$

will generate a group Q' of order p^p at least. This group does not contain S_{p-1}. The substitutions

$$S_{p-1}, \; BS_{p-1}B^{-1}, \; B^2S_{p-1}B^{-2}, \; \cdots, \; B^{p-1}S_{p-1}B^{-p+1}$$

and the group Q' will generate a group Q'' of order p^{2p} at least, etc. Finally, we have a group $Q^{(p)}$, of order $\geqq p^{p^2}$, linear in $V_1, V_2, \cdots, V_p$, which group with A and B generate a group of order $\geqq p^{p^2+2}$.

§ 20. Consider case (2). Constructing the substitutions

$$R_1 = BS_1B^{-1}, \qquad R_2 = S_1R_1S_1^{-1}R_1^{-1},$$

we find that R_2 is linear in $V_1, V_2, \cdots, V_p$, of rank 1 in V_1 and V_2 and of rank $\geqq 2$ in $V_3, V_4, \cdots, V_p$.

Now, S is linear in V_1 (§ 17). It cannot be linear in all the sets

V_2, V_3, $\cdots$, or S_1 would be linear throughout. Hence there is a substitution, $W = B^n S B^{-n}$, which is circular in V_1 and linear in V_2. Then the substitution $R_3 = W R_2 W^{-1} R_2^{-1}$ is linear in all the sets V_1, V_2, $\cdots$. It is of rank 2 in V_1 and of rank $\geqq 3$ in the remaining sets. Proceeding as in § 19, we construct a group $Q^{(p-2)}$ of order $\geqq p^{(p-2)p}$, linear throughout, a subgroup in the group generated by A, B and R_3. This group $Q^{(p-2)}$ and the substitutions R_2, BR_2B^{-1}, $B^2R_2B^{-2}$, $\cdots$ generate a group $Q^{(p-1)}$ of order $\geqq p^{p^2-p-1}$, linear throughout. This group and the substitutions S_1, BS_1B^{-1}, $B^2S_1B^{-2}$, $\cdots$ generate a group $\leqq Q_2$, of order $\geqq p^{p^2-1}$. Accordingly, the order of Q_3 is $\geqq p^{p^2}$.

The same processes, with slight variations, will dispose of case (3). Theorem III, α), will be found true.

§ 21. In proving Theorem III, β), we may assume that $Q_2 = P$.

There is a substitution $S' < Q_2$, but not $< Q_1$, which can take the place of S in Theorem I, Q_1 being substituted for P_1 in the theorem, and a corresponding group Q' taking the place of Q_1 in Theorems II and III, α). If $P = Q'$, Theorem III, β) is true. If $P > Q'$, then there exists a set of functions

$$V_1': \qquad y_1', \; y_2', \; \cdots, \; y_p',$$

corresponding to the set V_1 defined in § 17. These functions are permuted transitively by P; otherwise the order of this group would be $\geqq p^{p^2}$ [Theorem III, α)]. We will look upon P as transforming simultaneously the two sets V_1 and V_1', making use of the results of § 16.

We may evidently assume $S' = A$ of § 16. *Then A is linear and of rank 0 in V_1', and is circular in V_1.*

There must be a substitution A' which is circular in V_1'. We can evidently find an integer n such that the substitution $A'A^n$ is linear in V_1. Again, such numbers m and k can be found that the substitution

$$R = (A'A^n)^k S^m$$

is linear and of rank 0 in V_1 and is circular in V_1'.

The substitutions A and R will now generate a group of order $\geqq p^{2p-1}$. To prove this, we construct first $R_1 = ARA^{-1}R^{-1}$, which is linear and of rank 1 in both V_1 and V_1'; then the substitutions

$$R_2 = AR_1A^{-1}R_1^{-1}, \; R_3 = AR_2A^{-1}R_2^{-1}, \; \cdots,$$

which are all linear, of rank p in V_1', and of ranks 2, 3, $\cdots$, respectively, in V_1; finally, we construct the substitutions

$$W_2 = RR_1R^{-1}R_1^{-1}, \; W_3 = RW_2R^{-1}W_2^{-1}, \; W_4 = RW_3R^{-1}W_3^{-1}, \; \cdots,$$

all linear, of rank p in V_1, and of ranks 2, 3, 4, $\cdots$, respectively, in V_1'.

The substitutions R_1, R_2, R_3, $\cdots$; W_2, W_3, $\cdots$ will generate a group of order $\geqq p^{2p-3}$, linear in V_1 and V_1'. Again this group together with A and R will generate a group of order $\geqq p^{2p-1}$.

§ 22. Theorem IV is proved as follows. The invariant subgroup H_1 exists unless the condition $S(\pi) = \pi$ is satisfied (cf. § 6). But Theorems I, II and III were true in consequence of this condition.